EXHIBIT 1

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re Patent Application of: **Jen-Wei Kuo**
Serial No. 11/597,486
Filed: November 22, 2006
For: **Security Protection Apparatus and Method for Endpoint Computing Systems**

Confirmation No.: 6774
Group Art Unit: 2431
Examiner: Moorthy, Aravind K

BRIEF ON APPEAL

To the Commissioner of Patents and Trademarks
Mail Stop Appeal Brief - Patents
P. O. Box 1450
Alexandria, VA 22313-1450

Sir:

Please enter the following Brief on Appeal into the record.

Applicant is a small entity under 37 CFR 1.9 and 1.27.

Applicant hereby requests a two-month extension of time.

Pursuant to 37 C.F.R. § 41.20(b)(2), a check for the amount of $515 is enclosed as payment of the fee for filing the Appeal Brief as a small entity and the fee for 2 months extension beyond the 1 month allowed since the 1/14/2011 mailing of the Notice of Panel Decision from Pre-Appeal Brief Review.

CERTIFICATE OF MAILING / TRANSMISSION
I hereby certify that this correspondence is, on the date shown below, being deposited with the United States Postal Service with sufficient postage as Express mail in an envelope addressed to the
Commissioner of Patents
Mail Stop Appeal Brief – Patents
P.O. Box 1450, Alexandria, VA 22313-1450

Date: 4/11/2011

Respectfully submitted,

Jen-Wei Kuo
Applicant / Inventor

7005 Wilderness Road
Raleigh, NC 27613
Tel (919) 345-5700

04/13/2011 CCHAU1 00000016 11597486
01 FC:2402 270.00 OP

04/13/2011 CCHAU1 00000016 11597486
02 FC:2252 245.00 OP

Appeal Brief Under 37 C.F.R. § 41.37

TABLE OF CONTENTS

I. REAL PARTY IN INTEREST

The real party in interest for this application is Jen-Wei Kuo, the inventor of record.

II. RELATED APPEALS AND INTERFERENCES

None.

III. STATUS OF CLAIMS

Claims 1-3, 4, 7-9, 14, 18, 21-24, 27, 28, 33, 34, 36, 39, 45, 48, 65-69, 72-74, 90-92, 95, 98, 100, 102-104, 106-112, and 114-116 stand pending and rejected.

The rejections to Claims 1-3, 4, 7-9, 14, 18, 21-24, 27, 28, 33, 34, 36, 39, 45, 48, 65-69, 72-74, 90-92, 95, 98, 100, 102-104, 106-112, and 114-116 are here appealed.

IV. STATUS OF AMENDMENTS

None.

V. SUMMARY OF CLAIMED SUBJECT MATTER

The claimed subject matter of the application relates to the protecting of a network endpoint computing system ("endpoint") (Specification p1, lines 9 to 17; and Fig. 1B block 102) by using a hardware and software security subsystem (Specification p6 line 28 to p7 line 3; and Fig. 1B block 101) associated with the endpoint. The security subsystem resides "in or in close association with an endpoint, internally or externally connected with an endpoint as well as to a network". (Specification p6 line 28 to p7 line 3; and Fig. 1B block 101).

More specifically, the security subsystem provides its security functions to protect the host processor ("host") of the endpoint (Specification p1, lines 9 to 17; and Fig. 1B block 181):

> The word "endpoint" will be used here to refer to an "endpoint computing system", for example a computing system such as a server, a desktop or laptop PC, a PDA or a Smartphone, or a set-top box. The words "endpoint host" or "host" hereafter refer to a primary processor-based computing system supported by any primary operating system. Conventionally, one endpoint often comprises only one host, and in such case, a host is an endpoint, such as a conventional desktop PC, typically having a main processor, possibly one or more coprocessors, and typically running an operating system. Additional subsystems such as various peripherals, network interface devices, modems, etc, with or without their own operating systems, are sometimes connected to such endpoint hosts for a variety of purposes.

Independent claim 1 is directed toward: an apparatus associated with an endpoint (Specification p1, lines 9 to 17; and Fig. 1B block 102; p6 lines 28 to p7 line 3), and configurable between a network and a host (Specification p1, lines 9 to 17, and Fig. 1B block 181) of the endpoint, comprising computational resources, the computational resources at least comprising one processor, wherein the computational resources are not accessible by the host, are accessible over a secure connection by a management server (Specification p7, lines 23 to 32; and Fig. 1B block 103), and are configured to provide an open platform (Specification p11, lines 20 to 28; and Fig. 1B blocks 101, 108 and 109) able to execute security function software modules from multiple vendors (Specification p5, lines 1 to 4; and Fig. 1B blocks 151 to 191) and provide immunization (Specification p3, lines 15 to 20) and defense functionality (Specification p1, lines 21 to 26) to protect the host.

Independent claim 7 is directed toward: A hardware and software "security subsystem", also called a Security Utility Blade (SUB) (Specification p6, lines 28 to p7 line 3; Fig. 1B block 101), configurable between a network and a host of an endpoint, the security subsystem (SUB) comprising computing resources for providing: at least a plurality of immunization agent (Specification p12, lines 1 to 7, and Fig. 1B blocks 101 and 109) functions for providing immunization protection of the host; and an open platform (Specification p11, lines 20 to 28; and Fig. 1B blocks 101, 108 and 109) for receiving and executing security function software modules from multiple vendors for providing at least defense functions for protection of the host.

Independent claim 18 is directed toward: A computer system comprising a security subsystem (Specification p6, lines 28 to p7 line 3, and Fig. 1B block 101) and a host (Specification p1, lines 9 to 17; and Fig. 1B block 181) system, wherein the subsystem is connected between a network connection path and a bus of the host system; comprises a processor and additional computational resources, the processor executing at least a security-hardened operating system (Specification p9, lines 13 to 17); provides immunization and defense functions to protect at least the host system; is configured for access to resources of the host system and for preventing access from the host system to resources of the security subsystem; is configured for management access by a management server (Specification p7, lines 23 to 32; and Fig. 1B block 103) system; over a secure connection; and is configurable with security function software modules from multiple vendors (Specification p5, lines 1 to 4; and Fig. 1B blocks 151 to 191).

Independent claim 22 is directed toward: A security subsystem configurable between a network and a host of an endpoint, the security subsystem providing at least a plurality of immunization functions (Specification p3, lines 15 to 20) for immunization protection of the host; and comprising a processor and at least one of: a coprocessor, DSP, acceleration circuitry, reconfigurable circuitry, interface circuitry, data storage; and wherein the processor executes at least an operating system.

Independent claim 27 is directed toward: A security subsystem configurable between a network and a host of an endpoint, the security subsystem comprising computing resources for providing: an open platform (Specification p11, lines 20 to 28; and Fig. 1B blocks 101, 108 and 109) for receiving and executing security function

software modules from multiple vendors for providing defense functions (Specification p1, lines 21 to 26) for protection of the host.

Independent claim 33 is directed toward: A security subsystem configurable in the path of communications between a network and a host system of a network endpoint, the security subsystem comprising processing means at least for providing security for the host system, in part by executing security function software modules, wherein the processing means comprises at least: holding and executing means for at least one defense function software module for providing at least one defense function; and agent (Specification p12, lines 1 to 7; and Fig. 1B blocks 109) means for providing at least one immunization function.

Independent claim 48 is directed toward: A security subsystem comprising a processor and additional computational resources and associated with a network endpoint, wherein the security subsystem: is configurable in the path of communications between a network and a host system of the endpoint; is configurable to provide immunization and defense functionality for protecting the endpoint; is configurable either in or attached at the endpoint for communications via a bus of the host system for access to resources of the host system, so as to prevent access to resources of the security subsystem by the host system; is configurable for management access by a remote server (Specification p7, lines 23 to 32; and Fig. 1B, block 103) over a secure connection; and is configurable with security function software modules from multiple vendors. (Specification p7, lines 4 to 12; and Specification p5, lines 1 to 4; and Fig. 1B blocks 151 to 191)

Independent claim 65 is directed toward: A system for managing and providing security for at least one endpoint, the system comprising: at least one security subsystem associated with each at least one endpoint, each of the at least one security subsystems capable of being configured between a connecting network and a host of the respective endpoint; and a server (Specification p7, lines 23 to 32; and Fig. 1B, block 103) configured for communications with a database system (Specification p9, lines 18 to 20; and Fig. 1B block 104) and each of the at least one security subsystems; wherein each of the at least one security subsystems comprises at least a processor and operates to form an open platform capable of holding and executing multiple security software modules

for providing multiple security functions.

Independent claim 90 is directed toward: A security system for forming a management zone (Specification p7, lines 4 to 12; and Fig. 1B block 110) for at least one endpoint, the system comprising: an open platform processor-based security subsystem (SUB) at each of the at least one endpoints; a server (i.e. management server), (Specification p7, lines 23 to 32; and Fig. 1B block 103) in communications with a database system; wherein: each security subsystem is configured for communications with the server, and the management zone is characterized in that the server is configured to manage each security subsystem within the zone, so as to eliminate direct access by vendor security management systems (Specification p5, lines 1 to 4; and Fig. 1B blocks 151 to 191).

Independent claim 95 is directed toward: A method by a network-connected management entity of providing security function software modules to a network endpoint, comprising the steps of: downloading security function software modules from at least one security function vendor; storing the software modules in a database system (Specification p9, lines 18 to 20; and Fig. 1B block 104); and selecting and distributing at least one of the software modules, into a security subsystem (SUB) of the endpoint, the security subsystem (SUB) comprising: memory and a processor running an operating system and configured as an open platform for storing and executing security function software modules of multiple security function vendors.

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

The examiner has rejected Claims 1-3, 4, 7-9, 14, 18, 21-24, 27, 28, 33, 34, 36, 39, 45, 48, 65-69, 72-74, 90-92, 95, 98, 100, 102-104, 106-112, and 114-116 under 35 U.S.C. § 102(e) as anticipated by Lynn et al., U. S. Patent No. 7,058,796 B2.

VII. ARGUMENT

A. Claims 1-3, 4, 7-9, 14, 18, 21-24, 27, 28, 33, 34, 36, 39, 45, 48, 65-69, 72-74, 90-92, 95, 98, 100, 102-104, 106-112, and 114-116 are not anticipated under 35 U.S.C. § 102(e) by Lynn.

Appellant maintains that a prima facie case of anticipation of the pending claims has not been established because Lynn fails to disclose not just one but multiple elements, as arranged, in each of the independent claims.

It is not surprising that Lynn fails to disclose numerous claim features, because Lynn is not particularly relevant to the claimed invention, let alone novelty defeating. Lynn is directed toward an apparatus and method for a wireless area perimeter security system (see e.g. the Abstract of Lynn), wherein a security system listens and reacts to wireless traffic entering an area. In contrast, the application's claims specify a security apparatus connected between its endpoint and the outside world, i.e., specifically the endpoint's network connection, in order to protect the endpoint's host, e.g. its CPU or processor(s) (Specification p1, lines 9 to 17, and Fig. 1B block 181). The recited positioning of applicant's clamed security apparatus as "associated with an endpoint" is defined in the specification as "internally or externally connected with" the endpoint computer. (Specification p1, lines 9 to 17; Fig. 1B block 102; p6 line 28 to p7 line 3) This intimate positioning of the security system in association with its endpoint, among other novel features of the present invention, provide the claimed security apparatus numerous advantages in effectiveness over systems such as Lynn's and others in the prior art.

The comments above are background to the unusually extensive shortcomings of Lynn as anticipatory art to the claims at issue, as now detailed here below.

1. Claim 1 is Not Anticipated by Lynn.

a. Lynn does not teach an apparatus associated with an endpoint and configurable between a network and a host of the endpoint, comprising computational resources.

I.

Claim 1 recites "an apparatus associated with an endpoint and configurable between a network and a host of the endpoint." This feature comprises 1) the apparatus, which further in the claim is specified as providing security to its endpoint 2) the endpoint computer with which the

apparatus is associated, and 3) the relationship wherein the security apparatus is configurable between a network and endpoint host (e.g. processor-based computing system of, or comprising, an endpoint). The Examiner proposes (Final Office Action, p. 5) that Lynn teaches these features at Col. 8 lines 28-43 of Lynn. However, this passage only provides certain hardware components, i.e. devices 210A-D, which are further described in the passage as preferably mobile computer systems with at least wireless receivers, optionally wired connections to Ethernet 150 as well as peer-to-peer communications interfaces, and which in the aggregate may serve as the system processor of Lynn's security system, with storage that may or may not serve as the system data store (SDS) of the security system of Lynn. These devices, in other words, are merely part of the area defense system of Lynn. The relied upon passage fails to provide even one of 1) security apparatus providing security to its endpoint, 2) a protected endpoint computer, and 3) a security apparatus configurable between network and host of the protected endpoint.

The examiner however maintained, in the Final Office Action at p. 2, "Lynn discloses that the endpoints are (sic) the mobile computer systems such as a notebook computer." Applicant notes that for multiple reasons the mobile computers of Lynn cannot be the protected endpoints of Claim 1. First, the mobile computers (devices 210A-D) of the cited passage cannot provide the endpoint of claim 1 because they are actually *components of the security system* that is providing protection *to another entity*, a wireless area network, rather than being the entity receiving protection as called out in Claim 1. These mobile devices of the security apparatus of Lynn cannot at the same time be both *part of* the security system and *the object receiving* the security. Even if somehow it were granted that they could be both, the claim also calls in the ensuing line that the computational resources of the security apparatus are not accessible by the host, which would require that the apparatus not have access to itself, which seems quite unlikely to say the least.

Further, the mobile devices in the cited passage of Lynn have no security apparatus in association, that is, "internally or externally connected with an endpoint as well as to a network" as defined for the association relationship between the security apparatus and endpoint in Kuo's Specification p6, line 28 to p7 line 3, and Fig. 1B block 101 and specified in the claim limitation.

Thus the examiner erred in equating mobile computers of Lynn's security system, which are simply building blocks of Lynn's security system, with an end-user's endpoint or endpoint host, much less the entire three-fold claim element, because the mobile computers described in

Lynn a) are *part of* the security system, b) comprise no protected host within as required in the claim, and c) fail to provide an associated security apparatus configurable between host and network as recited in the claim. The cited portion of Lynn does not teach an apparatus associated with its endpoint and configurable between a network and a host of the endpoint as recited in Claim 1 for providing security to the host of the associated endpoint.

b. Lynn does not teach an apparatus wherein the computational resources are not accessible by the host.

Claim 1 recites, "wherein the computational resources are not accessible by the host." The examiner proposes (Final Office Action, p. 6) that Lynn provides this feature at Col. 8 L44 - Col 9 L3 of Lynn, and inserts parenthetically, after quoting from the claim, the words "i.e. SDS". The examiner appears to equate the SDS of Lynn with the applicant's "host". However, the SDS of Lynn is merely "a system data store capable of storing network default and configuration data" (Lynn Claim 1), and in addition is *part of the security system* of Lynn. The SDS is not a computing system, cannot provide security, is not associated with an endpoint, and is not the object of the protection as is the host – as is recited in claim 1. It appears that the examiner misunderstood the claim term "host", which is defined as noted above in applicant's specification at page 1, lines 9 to 17, and illustrated in Fig. 1B, block 181.

Regarding the main aspect of this claim feature, that the "computational resources are not accessible" by the host, the examiner provided nothing else. The claim limitation of ensuring that the computational resources of the security apparatus are "not accessible by the host" is absent from the relied-upon passage, and absent from Lynn because such a feature would not make sense in the context of Lynn's system.

Thus, the SDS is not the host, the claim limitation of preventing access by a protected endpoint host to the computational resources of the security system protecting it, as recited in Claim 1, and so the examiner erred and the rejection is improper.

c. Lynn does not teach an apparatus comprising computational resources, wherein the computational resources are accessible over a secure connection by a management server.

Claim 1 recites "wherein the computational resources are accessible over a secure connection by a management server." The Examiner failed to provide any indication of this feature in Lynn. The phrase "secure connection" does not appear in Lynn. Applicant contends that such a feature is neither taught or suggested anywhere in Lynn, and indeed would serve no logical purpose in a wireless area defense system such as Lynn's. Therefore Lynn does not teach a secure connection by a management server as recited in Claim 1, and so the examiner erred in rejecting over Lynn.

d. Lynn does not teach computational resources configured to provide an open platform able to execute security function software modules from multiple vendors.

Claim 1 recites, "wherein the computational resources are configured to provide an open platform able to execute security function software modules from multiple vendors." The Examiner proposes (Final Office Action, p6) that Lynn teaches this feature at Col 10 lines 17-29, and inserts in apposition to the claim limitation the phrase "(i.e. there are multiple independent data stores)". However, it is obvious that mere data stores "capable of storing network default and configuration data" (Lynn's Claim 1a) cannot constitute the claim limitation. The examiner failed to point out in Lynn *any* teaching of downloading of security function software modules from multiple vendors for execution by a computing system configured so as to provide open platform functionality. Multiple-vendor, open platform language is absent from Lynn, and Lynn lacks any teaching or suggestion of open platform capability.

Further, Lynn teaches in Col 31 Line 42-67 that the SDS is capable of storing network default and configuration data, indicating that Lynn's SDS is merely an element in a dedicated, closed system, not an open platform system which is able to execute software programs from various security software product vendors. (Specification p8 line 30 to p9 line 3; p11, lines 20 to 28; and Fig. 1B blocks 101, 108 and 109).

In the Final Office Action, on p. 5, the examiner argues, "The SDS downloads from the data store." However, the SDS *is* the data store, and furthermore a movement of data does not provide the feature of downloading or executing software modules from multiple vendors of software. Further, in the Final Office Action on p. 4 and again on p. 5, the examiner provides a definition of "open platform". Among other issues, applicant notes that the definition of "open

platform" provided by the examiner is faulty at least because it selectively omits critical portions such as the multi-vendor language even in the Wikipedia definition that the examiner appears to be quoting. The examiner's definition is conveniently so broad as to equate an open platform with practically any system.

For at least these reasons it is apparent that Lynn does not teach in the cited passage or elsewhere an apparatus that comprises an open platform able to execute security function software modules from multiple vendors as recited in Claim 1. Therefore, the rejection is improper.

e. Lynn does not teach computational resources configured to provide immunization and defense functionality to protect the host.

Claim 1 recites that the computational resources of the security system are "configured to provide immunization and defense functionality to protect the host." The examiner proposes (Final Office Action, p. 6) that this feature is taught in Lynn at Col 28 lines 33-41. The term "host" refers to the processor(s) or processing system within or constituting the protected endpoint with which the security apparatus is associated (Specification p1, lines 9 to 17; and Fig. 1B block 181). As defined and described in the specification, e.g. at paragraphs at p1, line 59, p5 line 3, and p7 L48, and as also known in the art, immunization functions are not defense functions, but are a different type of security functionality requiring different capabilities and thereby providing a different type of security. However, the cited passage of Lynn teaches only active defense mechanisms. Therefore, Lynn does not teach providing immunization and defense functionality as recited in Claim 1.

f. Lynn cannot anticipate Claim 1 because it does not teach all of the features of the claim.

As detailed above, Lynn fails to teach:

- An apparatus associated with an endpoint and configurable between a network and a host of the endpoint, comprising computational resources;
- That the computational resources are not accessible by the host;
- That the computational resources are accessible over a secure connection by a

management server;

- That the computational resources are configured to provide an open platform able to execute security function software modules from multiple vendors;
- That the computational resources are configured to provide immunization and defense functionality to protect the host.

All of these features are recited in Claim 1. As detailed above, each is absent from the examiner's relied-upon passages of Lynn. The system of Lynn is a system for defense of wireless area networks, and as a result it is hardly surprising that it bears little similarity to applicant's system, which, as specified in the claim language and consistently described in the specification, places applicant's claimed security apparatus between the host of an endpoint and its network connection.

As summarized concisely in MPEP § 2131, case law provides " 'A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference.' Verdegaal Bros. v. Union Oil Co. of California, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987)." (emphasis added). Also " 'The identical invention must be shown in as complete detail as is contained in the ... claim.' *Richardson v. Suzuki Motor Co.*, 868 F.2d 1226, 1236, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989)" (emphasis added). Moreover, "[e]very element of the claimed invention must be literally present, arranged as in the claim." *Id.* (emphasis added).

Lynn fails on multiple claim features. Therefore the applicant requests that the Board overturn the 35 U.S.C. § 102(e) rejection of Claim 1.

As Claims 2-3 and 4 depend on Claim 1, these rejections should also be reversed.

The remaining independent claims pending and currently rejected over Lynn have one or more similar features in common with the Claim 1 features argued above. In addition, these remaining independent claims in some instances also feature respective additional limitations that are absent from Lynn, as will be described below.

2. Claim 7 is Not Anticipated by Lynn.

Claim 7 recites several features that are similar to those of Claim 1 discussed above. For example, Claim 7 recites:

- a security subsystem configurable between a network and a host of an endpoint, the security subsystem comprising computing resources;
- providing immunization protection of the host
- an open platform for receiving and executing security function software modules from multiple vendors

For brevity, the arguments presented above with respect to Claim 1 will not be repeated. The Applicant submits that Claim 7 is allowable over Lynn for at least the same reasons as described above for Claim 1 for these similar features.

As Claims 8, 9, and 14 depend on Claim 7, these rejections should also be reversed.

3. Claim 18 is Not Anticipated by Lynn.

Claim 18 recites several features that are similar to those of Claim 1 discussed above. For example, Claim 18 recites:

> a subsystem is connected between a network connection path and a bus of the host system
>
> provides immunization and defense functions to protect at least the host system configured for management access by a management server system over a secure connection

For brevity, the arguments presented above with respect to Claim 1 will not be repeated. The Applicant submits that Claim 18 is allowable over Lynn for at least the same reasons as described above for Claim 1 for these similar features.

Additionally, as indicated in the first bullet-point above, Claim 18 recites in a manner more specific than Claim 1 that the security subsystem is connected to the bus of the host system. The examiner provided no indication of this claim element in Lynn (Final Office Action, p. 7). Due to the nature of the Lynn system as a wireless area security system as reviewed above regarding Claim 1, Lynn could not and so does not provide a security subsystem connected to a bus of the protected host system.

Additionally, Claim 18 recites "the processor executing at least a security-hardened operating system". The examiner proposes that Lynn teaches this feature at Col 10 line 63 to Col 11 line 4 (Final Office Action, p. 7). However, Lynn in the cited passage teaches only operating

systems, and provides no teaching or even a suggestion of awareness of or provision for the purposes that a hardened operating system would serve in such a security system as Lynn's. Therefore Lynn does not teach this feature of Claim 18, and thus the examiner erred in the rejection.

Multiple elements of Claim 18 are lacking in Lynn. Therefore the rejection should be reversed for Claim 18 and its dependent claims.

As Claim 21 depends on Claim 18, this rejection should also be reversed.

4. Claim 22 is Not Anticipated by Lynn.

Claim 22 recites features that are similar to the features of Claim 1 discussed above. For example, Claim 22 recites:

> a security subsystem configurable between a network and a host of an endpoint
> a security subsystem providing at least a plurality of immunization functions for immunization protection of the host

For brevity, the arguments presented above with respect to Claim 22 will not be repeated. The Applicant submits that Claim 22 is allowable over Lynn for at least the same reasons as described above for Claim 1 for these similar features.

As Claims 23 and 24 depend on Claim 22, these rejections should also be reversed.

5. Claim 27 is Not Anticipated by Lynn.

Claim 27 recites features that are similar to the features of Claim 1 discussed above. For example, Claim 27 recites:

> a security subsystem configurable between a network and a host of an endpoint, the security subsystem comprising computing resources
> an open platform for receiving and executing security function software modules from multiple vendors for providing defense functions for protection of the host

For brevity, the arguments presented above with respect to Claim 1 will not be repeated. The Applicant submits that Claim 27 is allowable over Lynn for at least the same reasons as described above for Claim 1 for these similar features.

As Claim 28 depends on Claim 27, this rejection should also be reversed.

6. Claim 33 is Not Anticipated by Lynn.

Claim 33 recites features that are similar to the features of Claim 1 discussed above. For example, Claim 33 recites:

> an open platform for receiving and executing security function software modules from multiple vendors for providing defense functions for protection of the host providing at least one immunization function.

For brevity, the arguments presented above with respect to Claim 1 will not be repeated. The Applicant submits that Claim 33 is allowable over Lynn for at least the same reasons as described above for Claim 1 for these similar features.

As Claims 34, 36, 39, and 45 depend on Claim 33, these rejections should also be reversed.

7. Claim 48 is Not Anticipated by Lynn.

Claim 48 recites several features that are similar to the features of Claim 1 discussed above. For example, Claim 48 recites:

> the security subsystem is configurable in the path of communications between a network and a host system of the endpoint
>
> configurable to provide immunization and defense functionality for protecting the endpoint
>
> configurable so as to prevent access to resources of the security subsystem by the host system
>
> configurable for management access by a remote server over a secure connection
>
> configurable with security function software modules from multiple vendors

For brevity, the arguments presented above with respect to Claim 1 will not be repeated. The Applicant submits that Claim 48 is allowable over Lynn for at least the same reasons as described above for Claim 1 for these similar features.

8. Claim 65 is Not Anticipated by Lynn.

Claim 65 recites several features that are similar to the features of Claim 1 discussed above. For example, Claim 65 recites:

> each of the at least one security subsystems capable of being configured between

a connecting network and a host of the respective endpoint

each of the at least one security subsystems comprises at least a processor and operates to form an open platform capable of holding and executing multiple security software modules for providing multiple security functions

The arguments presented above with respect to Claim 1 will not be repeated. The Applicant submits that Claim 65 is allowable over Lynn for at least the same reasons as described above for Claim 1 for these similar features.

Additionally, Claim 65 recites "the system comprising … a server configured for communications with a database system and each of the at least one security subsystems". The Examiner proposes (Final Office Action, p11) that Lynn teaches this feature at Col 10 lines 17-29, and inserts in apposition to the claim limitation the phrase "(i.e. there are multiple independent data stores)". Clearly, mere data stores cannot provide the claim limitation, and so the examiner erred. The applicant submits that Claim 65 is allowable over Lynn for at least this additional reason.

As Claims 66-69 and 72-74 depend on Claim 65, these rejections should also be reversed.

9. Claim 90 is Not Anticipated by Lynn.

Claim 90 recites features that are similar to the features of Claim 1 discussed above. For example, Claim 90 recites "an open platform processor-based security subsystem at each of the at least one endpoints." The arguments presented above with respect to Claim 1 will not be repeated. The Applicant submits that Claim 90 is allowable over Lynn for at least the same reasons as described above for Claim 1 for these similar features.

Additionally, Claim 90 recites forming a management zone, wherein "the management zone is characterized in that the server is configured to manage each security subsystem within the zone, so as to eliminate direct access by vendor security management systems." The Examiner proposes (Final Office Action, p14) that Lynn teaches this feature at Col 10 lines 17-29, and the examiner here again inserts in apposition to the claim limitation the phrase "(i.e. there are multiple independent data stores)". Leaving aside that the examiner has used the same paragraph on data stores for as teaching multiple different features, here again applicant maintains that no data stores of Lynn can constitute the claim limitation, and so the examiner erred. The applicant submits that Claim 90 is allowable over Lynn for at least this additional

reason.

As Claims 91 and 92 depend on Claim 90, these rejections should also be reversed.

10. Claim 95 is Not Anticipated by Lynn.

Claim 95 recites features that are similar to the features of Claim 1 discussed above. For example, Claim 95 recites that the security subsystem comprises "memory and a processor running an operating system and configured as an open platform for storing and executing security function software modules of multiple security function vendors." For brevity the arguments presented above with respect to Claim 1 will not be repeated. The Applicant submits that Claim 90 is allowable over Lynn for at least the same reasons as described above for Claim 1 for these similar features.

Additionally, Claim 95 recites a "method by a network-connected management entity of providing security function software modules to a network endpoint." The examiner provided no citation pointing out this limitation in Lynn, Lynn does not teach the feature, and therefore for this reason alone the rejection is improper.

Further, Claim 95 recites that the providing comprises the steps of "downloading security function software modules from at least one security function vendor; storing the software modules in a database system; and selecting and distributing at least one of the software modules, into a security subsystem of the endpoint." The Examiner seems to propose (Final Office Action, p15) that Lynn teaches each and all of these features (in addition to teaching numerous other quite different features as noted above) at the same short passage at Col 10 lines 17-29 of Lynn. Here again the examiner inserted in apposition to the claim limitations the phrase "(i.e. there are multiple independent data stores)". Clearly, however, no data stores can constitute any of these claim limitations, much less all of them. There is no teaching or suggestion in the cited passage of Lynn or elsewhere in Lynn that the data stores of Lynn's security system are used for storing security software modules from multiple vendors. There is no suggestion in Lynn of a system for doing so by a network-connected management entity as recited in Claim 95. For at least these reasons the examiner is shown to have erred and therefore the rejection of Claim 95 should be reversed.

As Claims 98, 100, 102-104, 106-112, and 114-116 depend on Claim 95, these rejections should also be reversed.

B. Argument Summary

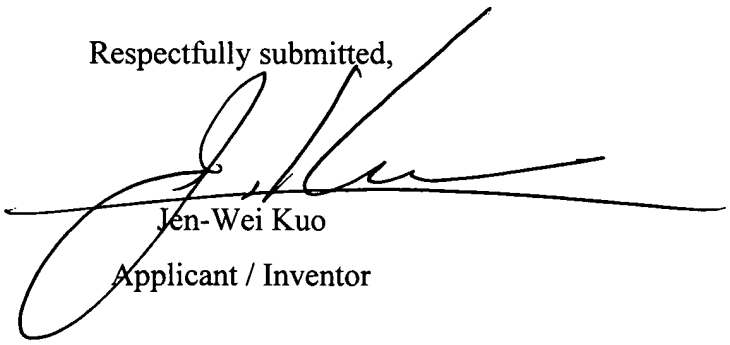
At a high level, the claimed invention of Kuo is patentably distinct from the system of Lynn. The claimed invention comprises a security apparatus intimately connected with, even residing within, its protected endpoint, while Lynn discloses a wireless area defense system loosely coupled to a wireless area network and with neither logical nor physical connections to protected end-user endpoint(s). Lynn fails to disclose multiple claim features of each independent clam because, at the outset, those features would make no sense in the system of Lynn.

At a lower level, the claim language recites numerous features that are absent from Lynn. For certain features the examiner provided no citations at all to Lynn. For multiple diverse claim features, the examiner cited to a same short paragraph of Lynn that fails to provide any of those features, much less all of them. Finally, not just one but multiple features and/or relationships between elements of each independent claim are simply absent from the examiner's relied-upon portions of Lynn. Thus the applicant submits that Lynn fails to anticipate the claims, and the rejection should be reversed.

VIII. CONCLUSION

For the above-stated reasons, it is submitted that the claims are in a condition for allowance. Applicant requests that the Board reverse the Examiner's rejection.

Respectfully submitted,



Jen-Wei Kuo
Applicant / Inventor

7005 Wilderness Road
Raleigh, NC 27613
Tel (919) 345-5700

IX. APPENDIX – CLAIMS

1. (Original) An apparatus associated with an endpoint and configurable between a network and a host of the endpoint,

comprising computational resources, the computational resources at least comprising one processor, wherein

the computational resources are not accessible by the host, are accessible over a secure connection by a management server, and are configured to provide an open platform able to execute security function software modules from multiple vendors and provide immunization and defense functionality to protect the host.

2. (Original) The apparatus of claim 1 wherein the computational resources comprise: receiving, holding, and executing means for the security function software modules; and agent means for supporting at least the immunization functionality.

3. (Original) The apparatus of claim 2 wherein the agent means comprise unified agent means comprising a plurality of sub-agents, traffic distributor functionality, data collection functionality, and action enforcer functionality.

4. (Canceled)

5. (Original) The apparatus of claim 1 wherein the endpoint comprises one of a desktop PC, a laptop or other PC, a workstation, a PDA, a cell phone, a smartphone, a set-top box.

6. (Canceled)

7. (Original) A security subsystem configurable between a network and a host of an endpoint, the security subsystem comprising computing resources for providing: at least a plurality of immunization agent functions for

providing immunization protection of the host; and an open platform for receiving and executing security function software modules from multiple vendors for providing at least defense functions for protection of the host.

8. (Original) The security subsystem of claim 7 wherein at least a subset of the plurality of immunization agent functions are provided using a unified agent.

9. (Currently amended) The security subsystem of claim [[7]] 8 wherein the unified agent comprises: a plurality of sub-agents, a traffic distributor, a data collector, an action enforcer, and a control and management plane.

10.-13. (Canceled)

14. (Original) The security subsystem of claim 7 wherein the endpoint comprises one of a desktop PC, a laptop or other PC, a workstation, a PDA, a cell phone, a smartphone, a set-top box.

15.-17. (Canceled)

18. (Original) A computer system comprising a security subsystem and a host system, wherein the subsystem is connected between a network connection path and a bus of the host system; comprises a processor and additional computational resources, the processor executing at least a security-hardened operating system;

provides immunization and defense functions to protect at least the host system; is configured for access to resources of the host system and for preventing access from the host system to resources of the security subsystem;

is configured for management access by a management server system over a secure connection;

and is configurable with security function software modules from multiple vendors.

19.-20. (Canceled)

21. (Original) The computer system of claim 18 wherein the processor and additional computational resources are configured to support a plurality of the following functions for supporting security functionality:

enabling control of the security subsystem and access to selected resources of the security system by an authenticated management entity over a secure channel; providing unified agent means comprising a plurality of sub- agents;

providing open platform functionality; providing network interface functionality for providing at least one of wireline and wireless network interface functions, where the network is an Ethernet, ATM, or wireless network, with connections to a private or public network; providing data stream inspection and treatment, to facilitate examination of at least incoming traffic, and facilitate selective treatment of the traffic based on at least one security function;

process traffic such that selected portions of incoming traffic are terminated at an isolator comprising "proxy" means, such that if selected portions of the incoming traffic pertain to predefined endpoint security management actions, the isolator routes the selected portions or representative signals to a unified agent for further processing; and

providing control and management plane functionality.

22. (Original) A security subsystem configurable between a network and a host of an endpoint, the security subsystem providing at least a plurality of immunization functions for immunization protection of the host; and comprising a processor and at least one of: a coprocessor, DSP, acceleration circuitry, reconfigurable circuitry, interface circuitry, data storage; and wherein the processor executes at least an operating system.

23. (Original) The security subsystem of claim 22 wherein the immunization functions are provided using a unified agent.

24. (Original) The security subsystem of claim 23 wherein the unified agent comprises a plurality of sub-agents, a traffic distributor, data collector, an action enforcer, and a control and management plane.

25-26. (Canceled)

27. (Original) A security subsystem configurable between a network and a host of an endpoint, the security subsystem comprising computing resources for providing:

an open platform for receiving and executing security function software modules from multiple vendors for providing defense functions for protection of the host.

28. (Original) The security subsystem of claim 27 further comprising computing resources for providing immunization agent functionality for protection of the host.

29.-32. (Canceled)

33. (Original) A security subsystem configurable in the path of communications between a network and a host system of a network endpoint, the security subsystem comprising processing means at least for providing security for the host system, in part by executing security function software modules, wherein the processing means comprises at least:

holding and executing means for at least one defense function software module for providing at least one defense function; and agent means for providing at least one immunization function.

34. (Original) The security subsystem of claim 33 wherein the processing means further comprises means for enabling control of the security subsystem and access to selected resources of the security system by an authenticated management entity over a secure channel.

35. (Canceled)

36. (Original) The security subsystem of claim 33 wherein the processing means further provide support for multiple security function software modules from multiple vendors for

providing multiple security functions as an open platform.

37.-38. (Canceled)

39. (Original) The security subsystem of claim 33 wherein the security subsystem is configured in or otherwise attached to the endpoint so as to provide direct access to computing resources of the host system via a bus or other means, while being configured to prevent access by the host system to resources of the security subsystem.

40.-44. (Canceled)

45. (Original) The subsystem of claim 33 wherein the processing means further comprises means for processing traffic such that selected portions of incoming traffic are terminated at an isolator further comprising "proxy" means, such that: if the selected portions of the incoming traffic pertain to predefined endpoint security management actions, the isolator routes the selected portions or representative signals to a unified agent for further processing.

46-47. (Canceled)

48. (Original) A security subsystem comprising a processor and additional computational resources and associated with a network endpoint, wherein the security subsystem:

is configurable in the path of communications between a network and a host system of the endpoint; is configurable to provide immunization and defense functionality for protecting the endpoint; is configurable either in or attached at the endpoint for communications via a bus of the host system for access to resources of the host system, so as to prevent access to resources of the security subsystem by the host system; is configurable for management access by a remote server over a secure connection; and is configurable with security function software modules from multiple vendors.

49-64. (Canceled)

65. (Original) A system for managing and providing security for at least one endpoint, the system comprising:

at least one security subsystem associated with each at least one endpoint, each of the at least one security subsystems capable of being configured between a connecting network and a host of the respective endpoint;

and a server configured for communications with a database system and each of the at least one security subsystems;

wherein each of the at least one security subsystems comprises at least a processor and

operates to form an open platform capable of holding and executing multiple security software modules for providing multiple security functions.

66. (Original) The system of claim 65 wherein the multiple security function software modules comprise at least one immunization function agent.

67. (Original) The system of claim 65 wherein at least a subset of the multiple security function software modules are from multiple vendors.

68. (Original) The system of claim 65 further providing a management zone wherein the security subsystem is maintained and defense and immunization functions are provided without interfering with end-user

processing.

69. (Original) The system of claim 65 wherein each of the at least one security subsystems further comprises a unified agent for supporting vendors' security management systems for multiple immunization functions.

70-71. (Canceled)

72. (Original) The system of claim 65 wherein the server carries out, via a control and management plane of each of the at least one security subsystems, at least one of provisioning, monitoring, and providing a control signal for at least one of the multiple security function software modules operating in each of the at least one security subsystems.

73. (Original) The system of claim 65, wherein the server comprises a unified interface converter configured for converting between vendor communications formats and a format used by the server, for communications with at least one vendors security management system.

74. (Original) The system of claim 65 wherein the server comprises at least one operator console, the console connected directly or over connecting networks to the unified interface converter.

75-89. (Canceled)

90. (Original) A security system for forming a management zone for at least one endpoint, the system comprising:

an open platform processor-based security subsystem at each of the at least one endpoints; a server in communications with a database system;

wherein: each security subsystem is configured for communications with the server, and the management zone is characterized in that the server is configured to manage each security

subsystem within the zone, so as to eliminate direct access by vendor security management systems.

91. (Original) The security system of claim 90 wherein the server is configured for providing at least one security function software module to each security subsystem, without direct access by a vendor security management system to the endpoint.

92. (Original) The security system of claim 90 wherein the server is configured to proxy for at least one immunization function by terminating and selectively proxying for vendor security management system communications, avoiding need for direct access into the zone by vendor security management systems.

93-94. (Canceled)

95. (Original) A method by a network-connected management entity of providing security function software modules to a network endpoint, comprising the steps of:

downloading security function software modules from at least one security function vendor; storing the software modules in a database system; and selecting and distributing at least one of the software modules, into a security subsystem of the endpoint, the security subsystem comprising:

memory and a processor running an operating system and configured as an open platform for storing and executing security function software modules of multiple security function vendors.

96-97. (Canceled)

98. (Original) The method of claim 95 wherein the management entity is a server for managing the provisioning of security function software modules for a plurality of security subsystems.

99. (Canceled)

100. (Original) The method of claim 95 further comprising the step of causing the security subsystem to receiveinformation originating from a billing and vendor information repository center, for making the information available to an endpoint user.

101. (Canceled)

102. (Original) The method of claim 95 wherein the database system is used to store at least one of endpoint information, auditing and forensic data, and defense function software modules, patches, and updates, through the coordination of a server.

103. (Original) The method of claim 95 wherein the security management systems fetch information from an endpoint or deposit data to an endpoint via the database system without directly accessing the endpoint.

104. (Original) The method of claim 95 wherein the database system serves one or multiple zones, each zone corresponding to at least one management entity.

105. (Canceled)

106. (Original) A server system for managing, over a connecting network, at least one processor-based security subsystem configured between the network and a corresponding endpoint host, each security subsystem providing the security functionality for the respective endpoint, the server system comprising:

data collection means, for collecting information from the at least one security subsystem;

data storing means, for storing at least a portion of the information into a database system;

action enforcing means, for receiving, terminating, and processing requests and other communications from at least a security management system.

107. (Original) The server system of claim 106 wherein each at least one security subsystem comprises an open platform, processor based security subsystem connected between the network and the host.

108. (Original) The server system of claim 106 wherein the security functionality comprises at least one type of immunization functionality for the endpoint.

109. (Original) The server system of claim 106 further comprising unified interface means for converting multiple vendor security management system communications formats into at least one format used within the server system.

110. (Original) The server system of claim 106 wherein the action enforcer means comprises a proxy function, the proxy function acting to interpret or translate requests from security management systems into a set of predetermined formats for communications between the server system and the at least one security subsystem.

111. (Original) The server system of claim 106 wherein the requests from the security management system pertain to applications comprising at least one of: patch management, configuration management, policy enforcement, vulnerability scan, sensitive data management,

asset management, password management.

112. (Original) The server system of claim 106 wherein the security management system obtains information related to a respective endpoint or deposits data intended for a respective endpoint to the database system under control by the server system.

113. (Canceled)

114. (Original) The server system of claim 106 wherein the database system is a repository for at least one of endpoint information, auditing and forensic data, defense function software modules, patches, and updates, through the coordination of the server system as assisted by a control and management plane of each of the at least one security subsystem.

115. (Original) The server system of claim 106 wherein the database system serves one or multiple zones of endpoints.

116. (Original) The server system of claim 106 wherein control and feedback means are provided between the server system and the connecting network over a connection to support functions such that security decisions of the server system can be disseminated via the connecting network for security-related actions comprising at least access control.

117. (Canceled)

X. EVIDENCE INDEX

None.

XI. RELATED PROCEEDING APPENDIX

None.